Diseño gráfico en la era *post-Snowden.* Criptografía tipográfica *y otros modos de camuflaje*

Dionisio Sánchez Rubio

Abstract

New surveillance modes imposed by governments and corporations is one of the biggest problems faced by contemporary society. The development of the Internet and the emergence of new technologies that make the monitoring of our data throughout the network possible, has led to a paradigm shift in the management of information, which directly affects our privacy. Faced with this situation we might wonder how the abuse of power to which we find ourselves subjected can be tackled and what we can do to open up a resistance zone that allows us to become aware of the problem.

Graphic designers, as cultural operators and generators of symbolic material, are making numerous contributions that question surveillance modes in the post-Snowden era. From critical design, speculative practices and activism, different projects have emerged which use typography and adopt encryption techniques to provide a critical view of social control that goes beyond any pragmatic or utilitarian use.

Our approach to these practices demonstrates the growing interest of graphic designers in the study of monitoring, seeing the connections between typography and privacy. To this end we have analysed the concept of social con-

trol and the impact it has on our society. Lastly, a study of the following projects has been carried out: *Project Seen* by Emil Kozole, ZXX by Sang Mun and *Typographic Obfuscation* by Chris Lange, given that they are crucial to understanding the relationship between encryption, steganography and typography.

Key words: *visual communication; encryption; surveillance; typography; steganography.*

Resumen

La nueva vigilancia impuesta por parte de gobiernos y corporaciones es una de las mayores problemáticas a las que se enfrenta la sociedad contemporánea. El desarrollo de Internet y la aparición de nuevas tecnologías que posibilitan la monitorización de nuestros datos en Red, ha propiciado un cambio de paradigma en la gestión de la información afectando directamente a nuestra privacidad. Ante esta realidad, cabe preguntarse cómo se puede hacer frente al abuso de poder al que nos vemos sometidos y qué podemos hacer para abrir un espacio de resistencia que nos permita tomar conciencia sobre la problemática.

Los diseñadores gráficos, como operadores culturales generadores de material simbólico, están realizando muchas aportaciones que cuestionan los modos de vigilancia en la era post-Snowden. Desde el diseño crítico, las prácticas especulativas y el activismo, han surgido diferentes proyectos que utilizan la tipografía y se apropian de las técnicas de encriptación, para aportar una mirada crítica sobre el control social que va más allá de posibles usos pragmáticos o utilitarios.

Nuestra aproximación a estas prácticas demuestra el creciente interés por parte de los diseñadores gráficos en los estudios sobre la vigilancia, viendo las conexiones entre tipografía y privacidad. Para ello hemos analizado el concepto de control social y las repercusiones que tiene en nuestra sociedad. Por último, se ha realizado un estudio de los proyectos *Project Seen* de Emil Kozole, ZXX de Sang Mun y *Typographic Obfuscation* de Chris Lange, pues son cruciales para poder entender la relación entre encriptación, esteganografía y tipografía.

Palabras clave: *comunicación visual; encriptación; vigilancia; tipografía; esteganografía*

1. Introducción

El desarrollo de Internet y de sus superestructuras, los avances tecnológicos (que han permitido mejorar las redes con una mayor velocidad de navegación y de transferencia de datos) y la democratización en los servicios (que ha sido posible gracias a la regulación de las tarifas), ha provocado un cambio en la gestión de la información a través de Internet creando, un mayor volumen de información que transita por la misma. A medida que han evolucionado las infraestructuras y el volumen de datos que estas registran, también ha habido un mayor interés por controlar la información, y tanto la empresa privada como los gobiernos se han dado cuenta de cómo utilizarlos para sus fines concretos.

Los datos que generamos en las redes sociales o el rastro que dejamos mientras navegamos por Internet es información que es clasificada y categorizada para detectar patrones de comportamiento o preferencias de consumo. Al aceptar las políticas de *cookies*, los acuerdos de licencia de determinados sitios web o las cláusulas cuando utilizamos los servicios de Facebook, Google o Amazon, damos el consentimiento para que nuestros datos puedan ser utilizados con fines comerciales y, al mismo tiempo. puedan ser cedidos al gobierno en caso de ser requeridos (El País, 2013). Esta situación ha creado una polémica sobre la vulnerabilidad de las leyes de privacidad que en muchos casos son insuficientes o hasta el momento no contemplan medidas específicas sobre el control de datos en Internet.

Desde 2012, la Comunidad Europea ha mantenido un intenso debate sobre cómo regular la protección de datos en el entorno digital. Tras varios años de controversia y bajo la presión de lobbies muy interesados en la gestión de la información, el Parlamento Europeo ha aprobado en abril de 2016 un paquete de medidas que "incluye nuevas normas mínimas sobre el uso de datos para fines judiciales y policiales" (Parlamento Europeo, 2016). Por consiguiente, muchas de las medidas tomadas han sido claramente insuficientes y un tanto ambiguas, al no hacer referencia explícita a las regulaciones del uso de la información por parte de las empresas, quedando patente los intereses que existen por parte de los diferentes grupos de presión.

A partir de las filtraciones de Wikileaks se ha creado un debate social sobre el control de la información y han sido muchas las voces que se han alzado para denunciar el abuso de poder por parte de organismos gubernamentales como la NSA (de sus siglas en inglés *National Security Agency*).

Los diseñadores, gráficos como productores de material simbólico, han reaccionado ante este problema con proyectos especulativos que intentan visibilizar los modos de ejercer el control sobre la información. En ese sentido, *Project Seen* de Emil Kozole, ZXX de Sang Mun y *Typographic Obfuscation* de Chris Lange, aportan una mirada diferente sobre la vigilancia al especular a través del diseño de tipografías posibles dispositivos capaces de evitar el rastreo de información en Internet. Independientemente de la operatividad de las tipografías diseñadas, los proyectos son una respuesta crítica sobre la vigilancia que explora la conexión entre diseño tipográfico y vigilancia, haciendo uso de técnicas propias de la vigilancia, como son la esteganografía o la criptografía.

La metodología utilizada en el estudio de los casos anteriormente mencionados se realiza a través de un análisis empírico, que nos ha permitido establecer sus aportaciones y limitaciones como dispositivos capaces de evitar el rastreo de información.

Para analizar el concepto de vigilancia y ver de qué manera opera en las sociedades de la información, se ha descrito de manera muy sintética cómo ha evolucionado el concepto de control social y vigilancia, examinando las implicaciones que tienen las nuevas formas de control en la sociedad contemporánea. Asimismo, se ha analizado el concepto de esteganografía y criptografía para poder entender mejor las técnicas utilizadas en los proyectos estudiados.

2. Vigilancia y Control Social

La vigilancia y el control social se han ejercido a lo largo de nuestra historia y sus métodos han ido cambiado de la misma manera que lo han hecho las estructuras sociales, transitando desde las sociedades disciplinarias que plantea Michel Foucault y las sociedades de control de Gilles Deleuze (Cortés, 2010), a nuevas formas de control social en las que los dispositivos de vigilancia y el poder que los ejerce son en todo momento inalcanzables (Bauman y Lyon, 2013).

Los dispositivos de vigilancia se han ido construyendo a lo largo del siglo XX a través de instrumentos de clasificación como son el documento de identidad, el registro de la huella dactilar, el control biométrico o el almacenamiento de datos (Deleuze, 2006; Bauman y Lyon, 2013; Mattelart y Vitalis, 2015); pero las nuevas formas de control se han vuelto cada vez más difusas gracias a los avances tecnológicos y el desarrollo de Internet a escala global. Durante ese proceso, la sociedad

ha ido asumiendo paulatinamente que la vigilancia y el control social son necesarios si queremos vivir en una sociedad más segura. La aceptación de los binomios libertad/privacidad – seguridad/control, ha provocado que la vigilancia se convierta en algo imperceptible y, por lo tanto, incontrolable.

Tal como señala Armand Mattelart en *Historia de la sociedad de la información*, (2002) autores como Gottfried Wilhelm Leibniz y sus coetáneos ya nos prevenían de la utilización de los algoritmos como una herramienta que permitiría "responder a las exigencias de la formación y del desarrollo del capitalismo moderno" (Mattelart, 2002, p.19), creando métodos especulativos de recogida de datos para usos empresariales.

Francisco Sierra Caballero, en su análisis sobre la obra de Armand Mattelart y André Vitalis: *De Orwell al cibercontrol* (2015), nos advierte de la insistente necesidad de "imponer y propiciar la devastadora lógica de dominio, o seguridad total, colonizando la esfera pública y extendiendo la política de la información de las «bellas mentiras» como relato único y verdadero de los acontecimientos históricos" (Sierra, 2015, p. 408).

Esa visión totalitaria que plantean Armand Mattelart y André Vitalis ha sido practicada por los gobiernos que utilizan la vigilancia como coartada para preservar la seguridad nacional. Los atentados del 11 de septiembre en Estados Unidos supusieron un punto de inflexión en relación con la vigilancia, induciendo a un estado de paranoia total en la ciudadanía. A partir de ese momento, el gobierno desarrolló leyes que le permitieron imponer un control sistemático de la información (Mattelart y Vitalis, 2015). El espectáculo del 11 de septiembre "ayudó a crear el sentimiento de amenaza que […] solo podía ser mitigado mediante nuevas medidas de seguridad y vigilancia" (Bauman y Lyon, 2013, p. 72). Un claro ejemplo de ese abuso de poder por parte de la jurisdicción de Estados Unidos es la Ley Patriota, que fue desarrollada e implementada a raíz de los atentados del 11 de septiembre y ha permitido al gobierno de los Estados Unidos solicitar información a las empresas con sede en el país o en cualquiera de sus filiales en todo el mundo (Whittaker, 2011).

A partir de ese momento, el mantra por razones de seguridad es utilizado en todos los dominios de la esfera pública, ya sea para controlar conflictos internacionales o para ejercer el control social en la ciudadanía. Esta situación ha sido definida por Agamben (2013) como un estado de excepción permanente que ha pasado de ser una medida aplicada, aplicada por los

gobiernos, a un estado normalizado que adquiere la forma de un continuo golpe de estado; desde entonces, los derechos de los ciudadanos se han visto vulnerados y la vigilancia se ha convertido en una estructura supranacional que se extiende a todos los ámbitos de la sociedad.

2.1. Vigilancia en la era post-Snowden

Las filtraciones de Edward Snowden a diferentes medios de comunicación en 2013, han sido determinantes para comprender el alcance que están ejerciendo gobiernos y empresas en el control de la información. Estos hechos han cambiado la percepción de la vigilancia en la ciudadanía, abriendo un debate sobre cómo estas medidas vulneran nuestro derecho a la privacidad (Lyon, 2014). Ahora nos vemos sometidos a una transparencia impuesta por la ideología Facebook, de la que participan gobiernos y empresas, pero esa transparencia sólo se da en un sentido, dado que:

> "La nueva vigilancia, basada en el procesamiento de la información […] permite una nueva transparencia en la que no solamente los ciudadanos como tal sino todos nosotros, en cada uno de los roles que asumimos en nuestra vida cotidiana, somos constantemente controlados, observados, examinados, evaluados, valorados y juzgados. Pero no ocurre lo mismo en el sentido contrario. A medida que los detalles de nuestra vida cotidiana se hacen más transparentes para los organismos que nos vigilan, más difícil resulta discernir cuáles son sus propias actividades" (Bauman y Lyon, 2013, p.21).

La información procesada es utilizada para controlar, evaluar y generar patrones que permiten la clasificación de la población en base a criterios establecidos y que responden a intereses corporativos e institucionales; de su clasificación se obtienen pautas que se pueden utilizar para hacer predicciones de comportamiento (Andrejevic & Gates, 2014).

2.2. Vigilancia y Cloud Computing

La información recogida en nuestras comunicaciones diarias, así como todos los documentos que alojamos en servidores de proveedores aparentemente gratuitos como Google Drive se almacenan en la nube, un lugar sin forma e intangible del que se conoce muy poco. La aparición del *Data Center* y su concepto intangible *Cloud computing*, se ha ido

desarrollando gracias a los avances tecnológicos que posibilitan la captación de grandes cantidades de datos y su posterior almacenamiento. Según Benjamin H. Bratton (2014), la nube puede entenderse como la nueva forma totalitaria adoptada por el estado, cuya ubicación exacta se mantiene en secreto bajo enormes medidas de seguridad y su transparencia se hace visible por medio de la mega-estructura que la contiene. Bratton sostiene que los diferentes sistemas y redes de la sociedad de la información están evolucionando de forma relacional constituyendo lo que él ha denominado *The Stack* (La Pila); un conjunto de capas (tierra, nube, ciudad, redes, interfase, dirección, usuarios), que se acumulan y dan forma a una estructura accidental que es aprovechada por los gobiernos con el único propósito de ejercer una vigilancia masiva a escala planetaria. La nube "extract revenue from the cognitive capital of their User-citizens, who trade attention in exchange for global infrastructural services that provide each of them a fixed and formal online identity and a license to use its services" (Bratton, 2015, p.110). Por consiguiente, nuestra relación con la nube es cada vez más compleja debido a que toda nuestra información se hace intangible y se desmaterializa: es transitoria y transita, y es a partir de ese momento cuando devenimos en datos susceptibles de ser controlados y almacenados.

La catalogación y almacenamiento de datos se realiza por medio de algoritmos y procesos de encriptación cada vez más sofisticados y discriminatorios. La evolución de las técnicas de encriptación ha ido condicionando los procesos y métodos utilizados en el control social; en ese sentido, la vigilancia y la criptografía mantienen una relación directa que sirve como base teórica a los proyectos de Emil Kozole, Sang Mun y Chris Lange, apropiándose de las técnicas de encriptación desde diferentes escalas de complejidad y operatividad.

2.3. Vigilancia, esteganografía y criptografía

La vigilancia y la criptografía están estrechamente conectadas debido a que siempre ha existido un interés por controlar información sensible que debía mantenerse en secreto por cuestiones políticas o militares. Esta información era transmitida por un medio de comunicación susceptible de ser interceptado y por lo tanto los mensajes podían ser descifrados; de esta necesidad por ocultar el contenido de los mensajes surge la criptografía. Los primeros ejemplos sobre la codificación de mensajes los encontramos en lo que se ha denominado esteganografía, una técnica que consiste en ocultar un mensaje dentro de otro.

El historiador griego Herodoto cuenta la historia de cómo los mensajeros griegos ocultaban los mensajes que tenían que entregar; para realizar esta tarea se afeitaban el pelo y escribían el mensaje en su cabeza, después se dejaban crecer el pelo y una vez en su destino se lo volvían a cortar para hacer de nuevo visible el mensaje a su receptor (Fernández, 2004). El problema en la utilización de este método es que los mensajes podían ser interceptados y descifrados, lo que provocó que las técnicas de encriptación evolucionaran hacia la criptografía, una técnica en la que los mensajes ya no estaban ocultos dentro de otros mensajes, ahora estos se codificaban para que solo aquella persona que conocía el código para descifrarlo pudiera leerlo. La principal diferencia entre criptografía y esteganografía estriba en que, mientras que la esteganografía oculta un mensaje dentro de otro mensaje, la criptografía no esconde el mensaje, más bien oculta su significado por medio de la codificación del mismo (Fernández, 2004); asimismo, el criptoanálisis es la ciencia que estudia los métodos para poder descifrar los códigos utilizados en la encriptación de un mensaje.

Durante las últimas décadas, y con la aparición de nuevos formatos de archivos digitales (audio, video, imagen), las técnicas de esteganografía se han hecho cada vez más sofisticadas y han permitido introducir mensajes ocultos sin cambiar la apariencia de los archivos en los que se alojan (Renza, et al., 2016). Un claro ejemplo es el *Block Pixel Hiding Method* (BPHM), un método muy utilizado que permite modificar las imágenes e introducir información dentro de las mismas.

Tanto la esteganografía como la criptografía han sido determinantes para el desarrollo de los proyectos que analizaremos posteriormente, al ser utilizadas de diferente forma y en distintos niveles de codificación.

3. Vigilancia desde el arte y el diseño gráfico

En el ámbito del arte, muchos artistas han explorado las consecuencias que tiene la vigilancia en nuestra vida cotidiana. Andrea Mubi Brighenti (2009) en su artículo *Artveillance: At the Crossroads of Art and Surveillance*, acuñó el término *Artveillance* para describir un conjunto de prácticas artísticas que tienen como eje comunicativo las nuevas formas de vigilancia. La visualidad y transgresión de estos proyectos ha suscitado el cuestionamiento sobre qué significa vivir en un estado de permanente vigilancia. El arte ofrece nuevos modos de entender la vigilancia desde una perspectiva que no suele ser abordada por los medios de comunicación.

La obra de Hito Steyerl es un claro ejemplo de esa interpretación

por parte de los artistas. Hito Steyerl en *How not to be seen: A Fucking Didactic Educational. MOV File* (2013) "alude, a través de una especie de tutorial para que una persona pueda llegar a ser invisible, al continuo seguimiento y vigilancia al que, según Steyerl, estamos sometidos desde hace años y cómo ese control ha ido en aumento sin que podamos hacer nada por remediarlo" (Duty-Free Art. Hito Steyerl, Anon., 2015).

De la misma forma, se han organizado muchas exposiciones que han tratado la problemática de la vigilancia en los últimos años. Es de especial relevancia la exposición *Astro Noise* de Laura Poitras, comisariada por Jay Sanders en febrero de 2016 en el museo Whitney de Nueva York. El título de la exposición hace referencia explícita a los documentos que Edward Snowden envío a Laura Poitras como prueba de las escuchas que estaba realizando la NSA.

En *Astro Noise* Laura Poitras ha intentado condensar todas sus inquietudes sobre el control social en la sociedad post-11S para mostrar e informar a una audiencia mayor los modos de operar de la NSA, hablando abiertamente sobre los mecanismos y términos en los que opera la vigilancia y así provocar una respuesta emocional a través de la experiencia estética del arte (Poitras, 2016).

3.1. Vigilancia desde el diseño gráfico

En el ámbito del diseño gráfico también existe una preocupación por investigar sobre las consecuencias políticas, sociales y culturales que tiene el estar vigilados constantemente; en ese sentido, el estudio de diseño gráfico Metahaven, es sin duda alguna, el que mayores aportaciones ha realizado a la investigación sobre la temática.

El trabajo de Daniel Van der Velden y Vinca Kruk actúa a dos niveles; por una parte, realizan un trabajo de investigación muy bien documentado sobre las problemáticas de la vigilancia y cuyos resultados finalmente son publicados en formato ensayo; y por otra, materializan esas ideas a través de propuestas visuales en las que Metahaven especula sobre otras narrativas por medio de escenarios ficticios, que se concretan en todo tipo de piezas gráficas, objetos y videos (Metahaven, 2015).

En su libro *Black Transparency. The Right To Know In The Age Of Mass Surveillance* (2015), Metahaven señala las revelaciones de Wikileaks como un momento clave en nuestra historia reciente, que ha provocado que el término transparencia —muy utilizado por los gobiernos como

sinónimo de la nueva democracia—, carezca de significado. Las filtraciones de Wikileaks son un punto de inflexión en relación con la transparencia, que ha generado un sentimiento de desconfianza general en la ciudadanía (Metahaven, 2015).

En *Black Transparency,* Metahaven analiza el problema de la computación en la nube, las superjurisdicciones desarrolladas por Estados Unidos, la propaganda pro-rusa en el conflicto con Ucrania y sus granjas de *likes* o la nueva guerra fría entre occidente y Rusia; todo ello por medio de una montaña de citas, referencias, memes, gráficos y diagramas, que hacen referencia a las realidades ocultas, metáforas, historias paralelas y mitos sobre el problema que existe a la hora de definir la transparencia.

3.2. Historias no contadas. Ruben Pater

Ruben Pater es un diseñador gráfico que trabaja en la vigilancia digital, en proyectos que él denomina *Untold Stories*, examinando la relación que existe entre el diseño gráfico y la política. Según Ruben Pater (Regine, 2015), el diseño gráfico permite crear un diálogo sobre las problemáticas sociales y políticas contemporáneas que, al igual que el arte o el periodismo, ayudan a comunicar estos problemas a audiencias más amplias.

Uno de sus proyectos sobre la vigilancia es *Spy Puzzles* (2014), una serie de puzles que se publicaron en el periódico holandés NRC Next en 2014 en forma de pequeños enigmas o micro-historias, que desvelan algunos de los métodos utilizados en los diferentes proyectos de vigilancia: la tecnología de reconocimiento facial, la vigilancia electrónica de países como Rusia, los drones o la encriptación.

En *The Drone Survival Guide* (2013) Ruben Pater especula sobre la creación de instrumentos que puedan evitar el rastreo de sensores de los drones. El proyecto consiste en el diseño de una guía en formato cartel que contiene las ilustraciones de los diferentes drones más utilizados por gobiernos y empresas privadas hasta la fecha. El póster cuenta con un manual de instrucciones que ha sido traducido a más de 15 idiomas, donde se explican algunos de esos métodos. *The Drone Survival Guide* es un proyecto especulativo que tiene relación con la propia materialidad del objeto; al estar impreso en papel metálico podría ser utilizado como una especie de parasol capaz de interferir en los sensores de los drones; pero tal y como señala el propio Ruben Pater (Pater, 2013), *The Drone Survival Guide* no es útil para la supervivencia y la lucha de aviones no tripulados y tampoco es una acción propagandística frente a este tipo de tecnologías. El proyecto más bien pretende informar a la población sobre el papel que tienen los drones en las zonas de conflicto armado y equilibrar la información sobre este tipo de tecnologías, ya que en muchas ocasiones desconocemos cuáles son los propósitos de las empresas y gobiernos que los utilizan; pero ¿Qué repercusión puede tener esta información frente a la imagen proyectada por los medios de comunicación? ¿De qué manera afectan estas propuestas a nuestra percepción sobre la utilización de los drones? El diseño gráfico puede ser entendido no solo como un instrumento que organiza determinada información en un contexto, sino como una alternativa para hacer frente a la información; el proceso de "diseñar" en este tipo de proyectos aporta al diseñador una nueva forma de entender la disciplina, su forma de abordar los problemas de sociedades en conflicto lo prepara para entender mejor determinados contextos socioculturales.
El trabajo de Ruben Pater o Metahaven —y el de otros muchos diseñadores como Reineke

Otten, Vincent Meertens, John Ryan, Matthieu Cherubini, Ekaterina Volkova y Iskra Vukšić, Anja Groten, Janna Ullrich o Simone C. Niquille—, demuestra el interés creciente por examinar las problemáticas sociales en relación a la vigilancia, el control de datos, las crisis migratorias o los estudios de género.

Figura 1. Portada del cartel guía de supervivencia contra drones: *Drone Survival Guide* de Ruben Pater (2013).

Figura 2. Parte trasera del cartel guía de supervivencia contra drones: *Drone Survival Guide* de Ruben Pater (2013).

4. Modos de camuflaje: tipografía, vigilancia y encriptación

La relación entre tipografía y criptografía se ha explorado en el diseño gráfico en proyectos donde se vincula la manipulación de la forma tipográfica con las técnicas de encriptación. En 2005, Samuel Luescher desarrolló *Disinter: Visual Encryption*, un proyecto que parte de la simplificación de la forma tipográfica como método de encriptación. Este método consiste en eliminar parte de los caracteres de la tipografía hasta hacerla totalmente ilegible, posteriormente si queremos visibilizar el mensaje, necesitamos tener una plantilla con las partes que han sido eliminadas y así poder ver el contenido del mensaje. Desde el mismo enfoque, Simon Thordal ha diseñado *Cryptex Typeface* (2015), una tipografía que estudia la relación entre criptografía y esteganografía a través del diseño de una fuente que, gracias a la simplificación de la forma tipográfica y la inclinación de determinados caracteres, provoca un efecto de confusión y dificulta la legibilidad del mensaje.

La diseñadora gráfica Allison Greenwald en *H(id)den* (2014) establece conexiones entre el cifrado, el lenguaje y la tipografía, reflexionando sobre los procesos opacos que hay detrás de las transacciones que realizamos diariamente con nuestros datos personales: números de contraseñas y tarjetas de crédito, fechas de nacimiento, códigos postales, licencias, pólizas, etcétera. Allison Greenwald procesa toda esta información y la visualiza por medio de diferentes técnicas de encriptación, que dan como resultado tipografías híbridas con un grado muy alto de abstracción.

Muy cercano a los planteamientos de Chris Lange en el uso de caracteres en formato Unicode, Luc Eggenhuizen ha diseñado *Cryptokey* (2015), una tipografía que puede ser utilizada para codificar textos. Aunque su funcionamiento es bastante complejo, Luc Eggenhuizen analiza las posibilidades que ofrecen los homoglifos del alfabeto de la tipografía Arial al vincularlos con los caracteres de la tipografía *Cryptokey*. Cada signo gráfico de la tipografía *Cryptokey* corresponde a dos o más signos gráficos de la tipografía Arial; al escribir un texto en Arial teniendo en cuenta las reglas de codificación propuestas por Luc Eggenhuizen, podemos decodificar el mensaje si cambiamos el estilo de fuente en el editor de textos de nuestro ordenador.

Estos ejemplos demuestran cómo los diseñadores gráficos están examinando las conexiones entre criptografía y tipografía; en muchas ocasiones, estos proyectos surgen en foros donde hackers, activistas y

diseñadores participan activamente para aunar tecnología, diseño y programación. En ese sentido, hay que destacar el *Crypto Design Challenge*, un evento que se celebró en el Museum of the Image en Breda (Holanda) en 2015, y que tuvo como objetivo convocar a diseñadores y artistas emergentes, para generar una imagen diferente de la *Deep Web* creando proyectos de investigación, que analizan los sistemas de vigilancia y el control en Internet a través del diseño de nuevos lenguajes de encriptación. En la actualidad, gracias al desarrollo de programas de diseño tipográfico es posible crear tipografías que pueden ser consideradas como activistas, al ser diseñadas como mecanismos de resistencia frente a los dispositivos que ejercen la vigilancia en Internet.

Desde esta lógica operan los casos de estudio que analizamos a continuación y cuya relación se establece desde planteamientos similares. Los tres proyectos analizados comparten el discurso y posicionamiento crítico frente a los dispositivos de control, al diseñar las tipografías por medio de aplicaciones digitales que intentan subvertir los mecanismos de control manipulando la forma tipográfica.

La tipografía es un pequeño software que se instala en nuestros ordenadores y por lo tanto permite que solo aquella persona que tiene la fuente instalada en su ordenador pueda ver el texto con la misma apariencia que nosotros. En ese sentido, la tipografía actúa como un mecanismo de encriptación basado en la esteganografía: oculta un mensaje dentro de otro (o una forma dentro de otra). Lo realmente interesante de este proceso es que al modificar la forma tipográfica podemos diseñar tipografías ilegibles en apariencia e imposibles de leer a simple vista, pero al tener la tipografía instalada en nuestro ordenador podremos decodificar el mensaje.

4.1. Tipografía Seen de Emil Kozole

Project Seen de Emil Kozole es un proyecto de investigación que analiza, a través del diseño de una tipografía, las conexiones que existen entre el lenguaje, los datos y la privacidad. Durante el desarrollo del proyecto, Emil Kozole estudió todas aquellas palabras que son sensibles a las búsquedas que realizan las organizaciones gubernamentales como la NSA y que suelen ser interceptadas en las comunicaciones que mantenemos diariamente; para ello, Emil Kozole ha creado una base de datos con las palabras más búsquedas en la monitorización de datos y ha analizado las herramientas que utilizan estas organizaciones para detectar las palabras. Posteriormente, la tipografía ha sido diseñada y programada con una

base de datos que permite reconocer determinadas palabras clave mientras escribimos; una vez detectadas, las tacha inmediatamente impidiendo su legibilidad. Asimismo, la tipografía cuenta con tres estilos de tachado que dificultan en mayor o menor medida la lectura de los textos: *Strikethrough, Blackout, Underlined*; además, al contar con un *plugin Bookmarklet*, la tipografía también puede ser utilizada cuando navegamos en Internet.

Pero la tipografía *Seen* en realidad no puede evitar el rastreo realizado a través de Internet, si utilizamos la tipografía en documentos con conversión PDF (del inglés *Portable Document Format*), el texto queda oculto en las capas del documento y puede ser leído como texto sin formato, siendo visible para determinados sistemas de rastreo de información e ineficaz como dispositivo de evasión del control.

4.2. Tipografía ZXX de Sang Mun

Partiendo del mismo planteamiento —la creación de una tipografía que evite el control de la información en Internet a través de un proceso de encriptación—, Sang Mun ha desarrollado una familia tipográfica que da forma a un proyecto especulativo sobre la vigilancia digital. Tras trabajar como agente de la NSA y participar en diferentes programas de vigilancia, se graduó como diseñador gráfico en la universidad Rhode Island School of Design con *ZXX* su proyecto final de carrera. Tal y como señala el propio Sang Mun (2013), su paso por la Agencia de Seguridad Nacional de los Estados Unidos ha influido en su trabajo como diseñador y le ha llevado a cuestionar los métodos que infringen nuestra privacidad en la sociedad actual. Bajo el nombre *ZXX* ha diseñado una tipografía que hace referencia a la normativa *Codes for the Representation of Names of Languages ISO 639.2*, una clasificación que incluye los códigos de representación de 21 idiomas que son utilizados para fines bibliográficos o de terminología. El código utilizado por Sang Mun está compuesto por tres caracteres que representan la abreviatura de una determinada lengua; en este caso el código se aplica para identificar textos sin contenido lingüístico: *"No linguistic content; Not applicable"*.

La familia tipográfica *ZXX* cuenta con seis estilos (*Sans, Bold, Camo, False, Noise* y *Xed*) que pueden intercambiarse entre sí para generar múltiples variantes. El diseño de la fuente en cada uno de sus estilos tiene pequeños elementos gráficos que alteran la forma tipográfica y dificultan su legibilidad; al modificar la apariencia de los caracteres, algunos sistemas de Inteligencia Artificial como el Reconocimiento Óptico de

Caracteres OCR (del inglés *Optical Character Recognition*) son incapaces de traducir la imagen a texto. A pesar de ser ilegible para los sistemas OCR, la fuente puede ser decodificada si el receptor tiene instalada la tipografía en su ordenador sirviendo como método de encriptación.

Al igual que la tipografía *Seen* de Emil Kozole, *ZXX* no es del todo operativa como dispositivo de evasión de monitorización de datos, esto se debe a que los documentos que enviamos con formato PDF pueden ser leídos al quedar el texto incrustado en las capas del archivo. En la figura 3 y 4 podemos ver textos escritos con la tipografía *Seen* y *ZXX* que han sido exportados en formato PDF; posteriormente se ha utilizado un lector OCR (se ha usado el software PDF OCR X para la conversión) y el traductor Google Translate para intentar descifrar los documentos. El lector OCR ha sido incapaz de leer las palabras tachadas con la tipografía *Seen* y tampoco ha podido descifrar el texto escrito con la tipografía *ZXX* (figuras 5 y 6). El motor de traducción de Google Translate no ha tenido ningún problema en decodificar ambos archivos, esto ocurre porque el lector OCR intenta trasladar la imagen a caracteres (no puede leer las capas de texto del documento PDF) mientras que Google Translate sí que puede leer el texto oculto en el documento PDF.

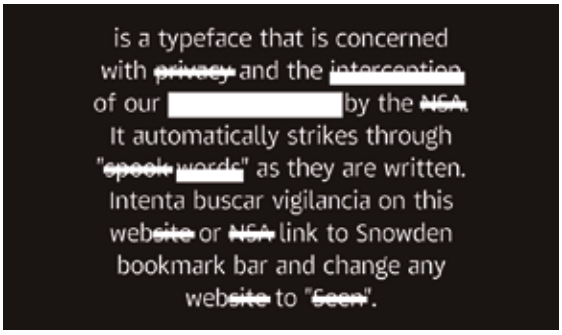

Figura 3. Texto escrito con la tipografía *Seen* diseñada por Emil Kozole en sus diferentes estilos: *Strikethrough, Blackout, Underlined*. Fotografía de producción propia.

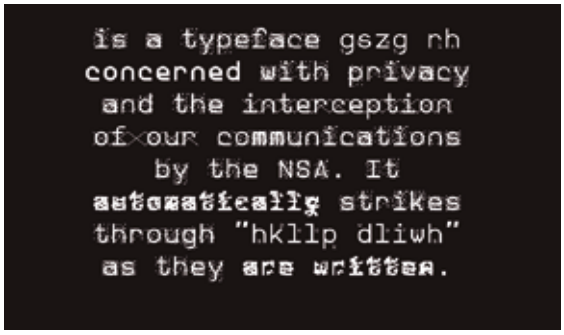

Figura 4. Texto escrito con la tipografía *ZXX* diseñada por Sang Mun en sus variantes *Sans, Bold, Camo, False, Noise* y *Xed*. Fotografía de producción propia

Figura 5. Imagen del archivo ".txt" de la interpretación de la tipografía *Seen* al pasar por el lector OCR. Fotografía de producción propia.

Figura 6. Imagen del archivo ".txt" de la interpretación de la tipografía *ZXX* al pasar por el lector OCR. Fotografía de producción propia.

4.3. Typographic Obfuscation de Chris Lange

El último proyecto analizado es *Typographic Obfuscation*, un trabajo de investigación realizado por Chris Lange en la OCAD University en Toronto por el que obtuvo el premio *Graphic Design Medal Winner* en 2014. Su investigación, que toma como punto de partida la creación de tipografías por medio del lenguaje de programación, se basa en el trabajo realizado por Donald Knuth, que desarrolló el lenguaje de programación MetaFont en 1979 para crear tipografías que se basan en el álgebra vectorial y la aritmética (Sinister, 2011).

El proyecto *Typographic Obfuscation* explora la legibilidad de las tipografías creadas con lenguaje de programación para ver de qué manera la modificación parametrizable de los caracteres posibilita el desarrollo de técnicas de encriptación. En su estudio, Chris Lange ha utilizado Metaflop, un software basado en el proyecto MetaFont de Donald Knuth desarrollado por Alexis Reigele (cofundador y desarrollador de Metaflop) y Marco Müller (diseñador gráfico de Metaflop y tipógrafo). Metaflop tiene un modulador con diversos parámetros que permite modificar la forma de la tipografía en: altura, anchura, altura de la x, altura de ascendentes y descendentes, etcétera. Una vez modificada la tipografía, podemos descargarla en nuestro ordenador y utilizarla en cualquier software de edición de textos. Al poder generar infinidad de variantes tipográficas por medio de Metaflop, se podría crear un conjunto de tipografías con determinadas variaciones que, combinadas entre sí, dieran como resultado textos escritos con fuentes al azar y crear patrones casi imposibles de descifrar (Lange, n.d). Existen muchos ejemplos de diseño de tipografías que utilizan el lenguaje de programación, pero lo realmente interesante de este tipo de técnicas es que nos permite especular sobre los posibles usos en el diseño de tipografías para evadir los mecanismos de control.

Tal y como señala Chris Lange (n.d), el uso de tipografías modificadas y alteradas no garantiza evitar su rastreo, ya que, como comentamos anteriormente, si utilizamos un archivo con formato PDF, el texto permanece oculto en sus capas. Para obtener una mayor eficacia frente al control toda nuestra comunicación debería realizarse a través de imágenes por ser mucho más difíciles de rastrear, a pesar de que su monitorización en redes sociales como Facebook o Instagram se realiza constantemente. Un ejemplo del uso de imágenes para evitar el rastreo de robots es el software CAPTCHA (del inglés *Completely Automated Public Turing test to tell Computers and Humans Apart*), un programa que protege de-

terminadas páginas web generando imágenes distorsionadas que suelen contener caracteres y números.

Chris Lange también estudia las posibilidades que ofrece la utilización de combinaciones de caracteres que tienen formas muy similares y, por lo tanto, son difíciles de diferenciar; a estos conjuntos de caracteres de apariencia homogénea se les denomina homoglifos y entre los homoglifos más comunes estaría el dígito cero y la o mayúscula (0 y O). Inspirado por el software CAPTCHA y por la utilización de homoglifos, Chris Lange explora las posibles combinaciones entre los diferentes glifos o caracteres de diversos idiomas en formato Unicode, para utilizarlos como una táctica de confusión —o de ofuscación si utilizamos el concepto de Lange—, capaz de dificultar la visión y evitar el descifrado. Al utilizar homoglifos en la escritura, obtenemos textos sin formato con una apariencia ilegible creada a partir de glifos que varían en grosor, espaciado, altura de la x o interletrado. Los textos escritos usando esta técnica siguen teniendo formato Unicode, pero su legibilidad es mucho más confusa. En la figura 8 se puede ver un texto escrito utilizando homoglifos que posteriormente se ha exportado en formato PDF y se ha usado un lector OCR y Google Translate para decodificarlo. El lector OCR no ha podido leer el texto y Google Translate tampoco ha podido traducir el texto a ningún idioma, tan solo algunas palabras sueltas (figuras 9 y 10). Los textos son visibles e incluso podemos llegar a reconocer determinados caracteres, pero su lectura se hace casi imposible de manera que el mensaje queda oculto y requiere un tiempo para poder ser descifrado por el receptor.

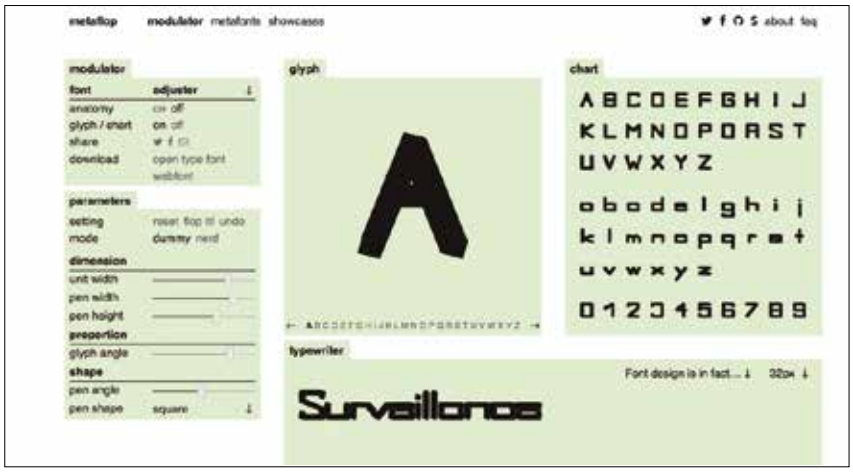

Figura 7. Imagen del software Metaflop.

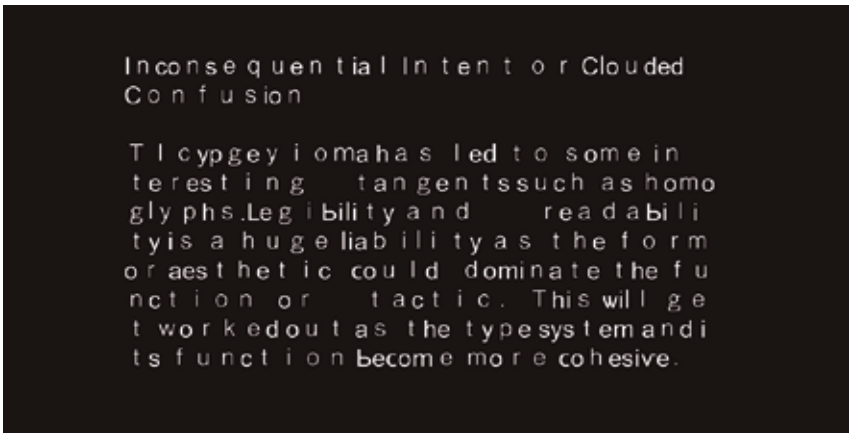

Figura 8. Imagen del texto escrito por Chris Lange utilizando homoglifos.

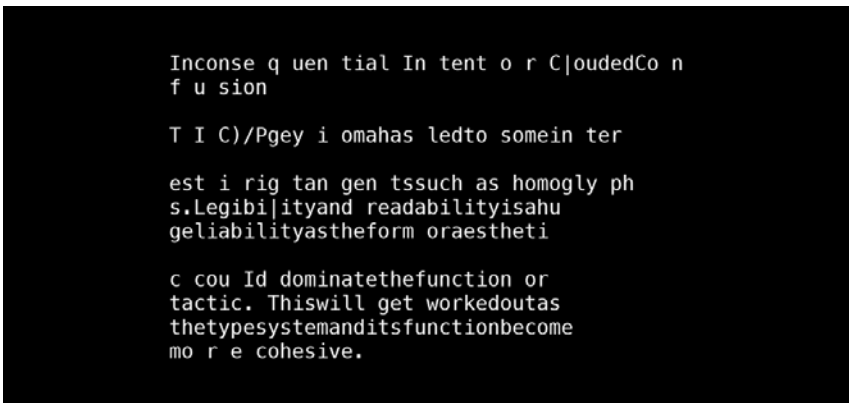

Figura 9. Imagen del archivo ".txt" de la interpretación al pasar por el lector OCR del texto escrito por Chris Lange utilizando homoglifos.

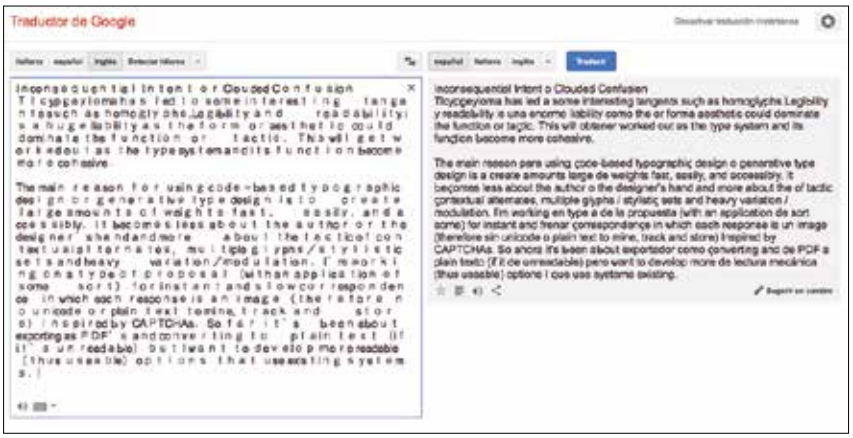

Figura 10. Imagen de la traducción de Google Translate del texto escrito por Chris Lange utilizando homoglifos.

5. Relación de operatividad en los casos estudiados

Del análisis de las tipografías podemos deducir que existen diferentes grados de operatividad/efectividad. La operatividad la relacionamos con la capacidad que tiene la tipografía como instrumento de evasión de control, y su efectividad nos muestra en qué grado lo consigue. A priori, el estudio revela que no se ha profundizado sobre el concepto de esteganografía como un sistema que pueda ser utilizado para evitar la monitorización de la información. Aun así, es evidente que las tipografías utilizan esta técnica y su operatividad así lo demuestra. Los textos escritos con las tipografías *Seen* y *ZXX* evidencian un grado de operatividad bajo/medio, ya que los párrafos escritos con estas fuentes llegan a ser visibles y en el caso de la tipografía *ZXX* podemos incluso llegar a intuir las formas de determinados caracteres.

Los casos se han planteado desde esa relación operatividad/efectividad. Por ejemplo, en el caso del diseño y programación de la tipografía *Seen* vemos que su operatividad es casi nula frente al software OCR y Google Translate; además, en su diseño y programación no se ha tenido en cuenta incluir palabras clave en otros idiomas que no fuera el inglés; por lo tanto, la tipografía solo es efectiva en determinados contextos de habla inglesa. El diseño de las tachaduras en sus diferentes variantes demuestra que Emil Kozole parece más interesado en los resultados estéticos que en los funcionales en el uso de la tipografía, ya que al escribir las palabras clave en sus diferentes estilos, vemos cómo algunas tachaduras no ocultan totalmente la palabra, por eso tiene un grado bajo de efectividad. También se puede apreciar la estudiada disposición de las tachaduras que demuestran que ha sido diseñada para crear ritmos visuales muy apropiados para el diseño editorial, dando la impresión de que su diseño responde a criterios meramente estéticos. A pesar de ello, hay que destacar que la tipografía actúa como un diseño conceptual en los términos propuestos por Anthony Dunne y Fiona Ruby (2013), como un diseño que escapa a la lógica del mercado para explorar nuevas ideas y hacer preguntas sobre el diseño, la política, la ética, la sociedad, y así sucesivamente.

En el caso de la tipografía *ZXX* de Sang Mun es evidente que sus conocimientos en relación con la vigilancia y su modo de operar son mucho más profundos, no solo por su experiencia como agente de la NSA, sino porque ha tenido en cuenta (y ha probado empíricamente) cómo reacciona frente a los sistemas de reconocimiento OCR. Pero el desarrollo de los diferentes estilos de dudosa necesidad y la extremada per-

formatividad en la presentación de los resultados revela que Sang Mun ha diseñado una familia tipográfica para diseñadores, algo que es muy común en el sentido de que el diseño tipográfico es una de las especializaciones de los diseñadores gráficos; pero los resultados arrojados en su análisis (que evidencian una operatividad media frente a los sistemas de reconocimiento OCR y una efectividad baja que depende del estilo que usemos) indican que no se ha profundizado en la búsqueda de un diseño tipográfico que aporte verdaderos mecanismos que eviten el rastreo de información en Internet.

Las tipografías *Seen* y *ZXX* se inscriben dentro del diseño especulativo y el diseño crítico (Dunne y Raby, 2013; Sueda, 2014; McCarthy, 2013) como propuestas visuales que tratan de hacer preguntas y abrir un debate sobre cómo opera la vigilancia en Internet. El diseño especulativo (discursivo, interrogativo, anti-diseño, diseño radical, etcétera) en muchas ocasiones tiene conexiones, influencias, tensiones, trasvases, con otras disciplinas y ámbitos de conocimiento. Los proyectos *Project Seen* y *ZXX* —al igual que el trabajo de Metahaven—, se ubican en un lugar difuso entre el diseño y el arte, que da como resultado propuestas visuales que en muchas ocasiones corren el peligro de ser proyectos que, en vez de enfocarse en las capacidades del diseño como una herramienta de transformación social e implicarse en la agenda política y social de manera profunda, se quedan en meros *shocks* visuales demasiado focalizados en un público privilegiado que utiliza el diseño especulativo o crítico para dar solución a las preocupaciones estéticas de una determinada élite intelectual (Mazé y Redström, 2009; Malpass, 2013; Bardzell y Bardzell, 2013; Prado y Oliveira, 2014).

En el caso de Chris Lange y su proyecto *Typographic Obfuscation* la relación operatividad/efectividad es mucho mayor. Su investigación realiza grandes aportaciones al estudio del diseño tipográfico con el fin de generar una herramienta o dispositivo para evitar (distorsionar, ofuscar, obstaculizar) la vigilancia en Internet. Su conocimiento sobre las técnicas de encriptación, como la esteganografía y la combinación de tipografías basadas en el lenguaje de programación, aporta una nueva mirada a la relación muy poco explorada entre tipografía/encriptación que deja entrever posibilidades de evasión del control a través de la manipulación de la forma tipográfica. La combinación y programación de tipografías basadas en la teoría de Chris Lange propone nuevas vías de investigación a explorar en las que se puede añadir la variable tiempo, creando tipografías que puedan mutar constantemente entre emisores y receptores (algunos ejemplos, como el desarrollado por Second Thou-

ghts en su web diseñada y programada por Chris Hamamoto y Chris Lewis, señalan de forma muy básica en esa dirección). También se podrían incluir algoritmos de encriptación en el software de la tipografía o desarrollar un software que permita realizar combinatorias automatizadas para crear fuentes tipográficas aleatorias mientras escribimos. Una idea similar es aplicada a la identidad visual desarrollada por Dexter Sinister para la Galería Kadist, donde la tipografía del logotipo cambia cada año gracias a las múltiples variantes desarrolladas de forma aleatoria en Metaflop.

La innovación en los planteamientos de Chris Lange se sustenta en su alto grado de operatividad/efectividad, y es operativa en el sentido de que cumple con su función como un instrumento que evita el monitoreo de información con un grado de efectividad muy alto; además, su tesis abre nuevos caminos para investigar la relación entre tipografía/criptografía, haciendo uso de herramientas de creación y programación de fuentes.

6. Conclusiones

Es evidente que la vigilancia evolucionará hacia nuevas formas de control cada vez más complejas y discriminatorias. Los nuevos algoritmos entrenados para distinguir los rasgos raciales en el reconocimiento facial, las clasificaciones que se basan en datos estadísticos que se extraen de nuestras interacciones en las redes sociales o la utilización de procedimientos cuánticos en los métodos de encriptación provocan una enorme preocupación sobre las consecuencias que tendrán estas tecnologías de clasificación, perfilando un futuro incierto sobre qué significará la privacidad, la seguridad, el control o la libertad.

Al mismo tiempo, desconocemos las consecuencias que tendrá la computación en la nube a escala global, algo que será determinante en función de sus capacidades limitadas por saturación y magnificación. Esta situación puede provocar restricciones en los servicios basados en la nube, que pueden dar lugar a nuevas formas

de exclusión social y crear una profunda asimetría en el acceso a contenidos en Internet; por lo tanto, es pertinente preguntarse por el papel que desempeñarán los diseñadores en el futuro y cómo responderán ante esta nueva realidad.

La verdadera importancia de los proyectos estudiados es que revelan la problemática sobre la vigilancia digital y la ponen en la superficie para advertirnos de sus consecuencias; al mismo tiempo, proponen alternativas basadas en la investigación-experimentación sobre las técnicas de evasión del control que tratan de hacer preguntas tanto desde su aplicación práctica como desde su valor simbólico sobre el control social y sus mecanismos, proponiendo nuevos horizontes desde donde el diseñador gráfico puede implicarse en la agenda política a nivel global (Mun, 2013).

Una de las principales aportaciones de los proyectos analizados es que evidencian la autonomía del diseñador (como autor, productor, activista, mediador, etcétera) al posicionarse de forma crítica frente a la problemática de la vigilancia. A diferencia de otras formas de activismo donde se trabaja colectivamente, aquí es el diseñador el que toma la iniciativa apropiándose de las técnicas inherentes a la vigilancia. Una segunda particularidad la encontramos en el uso de la tipografía, si tradicionalmente el papel de la tipografía en el activismo ha sido pasivo —como un elemento que posibilita la comunicación en determinados mensajes visuales: gráfica propagandística, carteles o folletos—; aquí adquiere un papel activo, ya que las fuentes diseñadas interactúan con los mecanismos de vigilancia impidiendo que los mensajes puedan ser descifrados.

Los proyectos expuestos constatan que cada vez hay más diseñadores gráficos interesados en la investigación crítica para desarrollar su práctica profesional de forma autónoma; este nuevo marco disciplinario, que va desde la noción tradicional del concepto de diseño a una nueva forma de entender la disciplina (algunos autores como Ezio Manzini han definido esta transición como diseño emergente), abre nuevas posibilidades para crear un entorno más favorable desde donde desarrollar narrativas y futuros escenarios a través del diseño.

Los proyectos aquí analizados cuestionan cuál es la función y la responsabilidad del diseñador más allá de los límites tradicionales de la disciplina, y esa es la verdadera cualidad que nos gustaría destacar. Además, tal y como señala Saskia Van Stein (2016) o Ramia Mazé (2014), el desarrollo de la tecnología y su apropiación por parte de los diseñadores

posibilita nuevos procesos, sistemas y estrategias de diseño, que dan forma a nuevas realidades que suelen estar ocultas. El diseñador *emergente* debe cuestionar cómo se conforma nuestra sociedad, para intentar dar visibilidad a problemas tan complejos como son la libertad de información, la transparencia o la vigilancia digital.

Dionisio Sánchez Rubio
Graduado en diseño por la Escuela de Arte y Superior de Diseño de Valencia (EASD) y Máster en Producción Artística por la Universitat Politècnica de València. En la actualidad está cursando el Máster en Artes Visuales y Multimedia en la Universitat Politècnica de València, es Personal Investigador en Formación en el grupo de investigación Laboratorio de Creaciones Intermedia del Departamento de Escultura en la Universitat Politècnica de València, y Doctorando en Arte: producción e investigación en la Universitat Politècnica de València. Es investigador en el proyecto "Recuperación de prácticas pioneras del arte de acción de la vanguardia histórica española y su contribución a la historia de la performance europea" financiado por proyectos de I+D "excelencia" y Proyectos de I+D+I "Retos Investigación". Ha colaborado en el grupo de investigación "Grupo de Estudios sobre Violencia de Género" en el proyecto: "Disculpen las molestias el machismo mata", financiado por el Ministerio de Educación, Cultura y Deporte. Desde el 2012 es profesor invitado en la asignatura "Color en los espacios públicos. Video Mapping y nuevas tecnologías del color "en el Grado en Diseño Industrial de la Universitat Politècnica de València.
E-mail: dioni.grafico@gmail.com

Referencias

Alonso, N., 2016. Estados Unidos tiene registrados los rostros de la mitad de sus ciudadanos. *El País* [online] Disponible en: <http://internacional.elpais.com/internacional/2016/10/20/estados_unidos/1476996646_669203.html> [Fecha de consulta: 5 de noviembre de 2016].

Andrejevic, M., Gates, K., 2014. Big data surveillance: Introduction. *Surveillance & Society*, 12(2), 185-196.

Agamben, G., 2013. For a theory of destituent power. *Critical Legal Thinking* [online] Disponible en: <http://criticallegalthinking.com/2014/02/05/theory-destituent-power/> [Fecha de consulta: 6 de julio del 2016].

Bardzell, J., Bardzell, S., 2013. What is "Critical" about Critical Design? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3297-3306). ACM.

Baudrillard, J., 1982. *Crítica de la economía del signo*. México: Editorial SIGLO XXI.

Bauman, Z., Lyon, D., 2013. *Vigilancia líquida*. Barcelona: Paidós.

Bernal Martín, M. J., 2016. Reseña: "De Orwell al cibercontrol", de Armand Mattelart y André Vitalis. *Caracteres. Estudios culturales y críticos de la esfera digital,* 5(1), pp. 191-255.

Bratton, B.H., 2016. *The stack: On software and sovereignty*. Cambridge: The MIT Press.

Bratton, B., 2014. The Black Stack. *E-Flux Journal*. [online] Disponible en: <http://www.e-flux.com/journal/the-black-stack/> [Fecha de consulta: 3 de julio del 2016].

Brighenti, A. M., 2009. Artveillance: At the crossroads of Art and Surveillance. *Surveillance & Society*, 7(2), pp. 175-186.

Caballero, F. S., 2016. De Orwell al cibercontrol (A. Mattelart y A. Vitalis). Chasqui. *Revista Latinoamericana de Comunicación*, (130), pp. 404-408.

CAPTCHA, n.d. CAPTCHA. [Online] Disponible en: <http://www.captcha.net> [Fecha de consulta: 23 de agosto del 2016].

CCCB, 2012. *Ciudadanía, Internet y democracia. Crítica de Facebook y medios sociales alternativos*, Conferencia de Geert Lovink (noviembre, 2012), Centre de Cultura Contemporània de Barcelona Videos [online]. Disponible en: <http://www.cccb.org/es/multimedia/videos/ciudadania-internet-y-democracia-critica-de-facebook-y-medios-sociales-alternativos/211283> [Fecha de consulta: 25 de mayo del 2016].

Chapman, C., 2015. This Font Lets You See if You're on the NSA's Radar. *The Creators Project,* [online] Disponible en: <http://thecreatorsproject.vice.com/blog/this-font-lets-you-see-if-you-re-on-the-nsas-radar> [Fecha de consulta: 2 de agosto del 2016].

Citizenfour. 2015 [DVD] Laura Poitras. Estados Unidos: Piffl Medien.

Cryptodesign, n.d. *Cryptodesign*. [Online] Disponible en: <https://cryptodesign.org> [Fecha de consulta: 21 de noviembre del 2016].

Cortés, J.M.G., 2010. *La ciudad cautiva: Orden y vigilancia en el Espacio Urbano*. Madrid: Ediciones AKAL.

Connor, M., 2013. Hito Steyerl's "How Not to be Seen: A Fucking Didactic Educational. MOV File". *Rhizome Journal*, [online] Disponible en: http://rhizome.org/editorial/2013/may/31/hito-steyerl-how-not-to-be-seen/ [Fecha de consulta: 2 de agosto del 2016].

Deleuze, G., 2006. Post-scriptum sobre las sociedades de control, *Polis* [online] Disponible en: <http://polis.revues.org/5509> [Fecha de consulta: 25 de mayo del 2016].

Dunne, A., Raby, F., 2013. *Speculative Everything: Design, Fiction, and Social Dreaming*. Cambridge: The MIT Press.

EL PAÍS, 2013. *Sanción a Google por vulnerar derechos del ciudadano*. [Online] Disponible en: <http://tecnología.elpais.com/tecnologia/2013/12/19/actualidad/11387450618_053467.html> [Fecha de consulta: 23 de mayo del 2016].

Eggenhuizen, L. 2015. *CryptoKey.* [Online] Disponible en:
<http://www.luceggenhuizen.com/cryptokey.html>
[Fecha de consulta: 21 de noviembre del 2016].

Eikvil, L., 1993. Optical character recognition. *Academia.edu* [Online]
Disponible en:
<http://s3.amazonaws.com/academia.edu.documents/33085443/
OCR.pdfAWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Ex-
pires=1472814713&Signature=jexeefbcYkGJgI3GdEWxIi5%2Bjo-
c%3D&response-content-disposition=inline%3B%20filename%3DO-
CR_Optical_Character_Recognition_OCR_-O.pdf>
[Fecha de consulta: 11 de junio del 2016].

Fernández, S.F., 2004. La criptografía clásica. *Sigma: revista de matemá-
ticas= matematika aldizkaria*. [Online] Disponible en:
<http://s3.amazonaws.com/academia.edu.documents/40562076/9_
Criptografia_clasica.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMT-
NPEA&Expires=1472803062&Signature=f8X3E5KF1yw1TPzjyta-
X%2B6tidzA%3D&response-content-disposition=inline%3B%20file-
name%3DCriptografia_clasica.pdf>
[Fecha de consulta: 22 de junio del 2016].

Foucault, M., 1990. *Vigilar y castigar: nacimiento de la prisión*
(trad. Aurelio Garzón del Camino). Madrid: Siglo XXI.

Galende, J. C., n.d. *Elementos y sistemas criptográficos en la escritura
visigótica*. [pdf] Universidad Complutense de Madrid. Disponible en:
<https://www.ucm.es/data/cont/docs/446-2013-08-22-9%20juanc.pdf>
[Fecha de consulta: 23 de abril del 2016].

Greenwald, A., 2014. *h(id)den*. [Online] Disponible en:
<http://www.allisongreenwald.com/installation/>
[Fecha de consulta: 21 de noviembre del 2016].

Gil, A., 2015. *Criptografía: la evolución algorítmica de la seguridad*
[online] Disponible en:
<https://hipertextual.com/2015/03/criptografia-seguridad>
[Fecha de consulta: 4 de noviembre del 2016].

Grandsire, C., 2004. *Metafont tutorial.* [pdf] Disponible en:
<http://metafont.tutorial.free.fr/downloads/mftut.pdf>
[Fecha de consulta: 3 de agosto del 2016].

Guerra, C., 2015. Los mundos posibles de Hito Steyerl. En: *Hito Steyerl Duty-Free Art*. Madrid: Museo Nacional Centro de Arte Reina Sofía.

ISO 639-2, 2014. *Codes for the Representation of Names of Languages ISO 639.2*. ISO 639-2. [online] Disponible en: <https://www.loc.gov/standards/iso639-2/php/code_list.php> [Fecha de consulta: 2 de agosto del 2016].

Kozole, E., n.d. *Project Seen*. [Online] Disponible en: <http://emilkozole.com/Project-Seen> [Fecha de consulta: 26 de julio del 2016].

Kozole, E., n.d. *Temporary Haven*. [Online] Disponible en: <http://temporaryhaven.tumblr.com> [Fecha de consulta: 26 de julio del 2016].

Quijano, P. R., 2015. Desafíos de la acción colectiva en la era post-Snowden: lecturas desde América Latina. *Teknokultura* [online] Disponible en: <http://revistas.ucm.es/index.php/TEKN/article/view/51340> [Fecha de consulta: 24 de junio del 2016].

Hanrahan, J., 2014. The Drone Survival Guide Explains How to Take Down Flying Robots. *Vice Magazine*, [online] Disponible en: <http://www.vice.com/read/drone-survival-guide-ruben-pater-interview> [Fecha de consulta: 24 de mayo del 2016].

Lange, C., n.d. *Chris Lange*. [Online] Disponible en: <http://www.chrislange.ca> [Fecha de consulta: 28 de julio del 2016].

Lange, C., n.d. *Thesis: Type & Obfuscation*. [Online] Disponible en: <http://recentactivity.tumblr.com> [Consultado 28 de julio del 2016].

Lyon, D., 2014. Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society,* 1(2). [e-journal] Disponible en: <http://bds.sagepub.com/content/1/2/2053951714541861.short> [Fecha de consulta: 23 de junio del 2016].

Parlamento Europeo, 2016. *Reforma de la protección de datos – Nuevas reglas adaptadas a la era digital.* [Online] Disponible en: <http://www.europarl.europa.eu/news/es/news-room/20160407I-PR21776/reforma-de-la-protección-de-datos-nuevas-reglas-adaptadas-a-la-era-digital>
[Fecha de consulta: 2 de junio del 2016].

Paredes, G., 2006. Introducción a la Criptografía. *Revista Digital Universitaria* [online]
Disponible en: <http://www.revista.unam.mx/vol.7/num7/art55/jul_art55.pdf>
[Fecha de consulta: 22 de junio del 2016].

Pater, R., 2014. *Puzzled by Espionage*. [Online] Disponible en: <http://www.untold-stories.net/?p=Puzzled-by-Espionage>
[Fecha de consulta: 1 de agosto del 2016].

Pater, R., 2013. *Twenty-first Century Birdwatching*. [Online] Disponible en: <http://www.untold-stories.net/?p=Drone-Survival-Guide>
[Fecha de consulta: 1 de agosto del 2016].

Pater, R., 2015. *The Sounds of Violence*. [Online] Disponible en: <http://www.untold-stories.net/?p=The-Sounds-of-Violence>
[Fecha de consulta: 1 de agosto del 2016].

Poitras, L., Sanders, J., Boumediene, L., Doctorow, C., & Crawford, K., 2016. *Astro Noise: A Survival Guide for Living Under Total Surveillance*. New York: Whitney Museum of American Art / Yale University Press.

Prado, L., Oliveira, P., 2014. Questioning the 'critical' in Speculative & Critical Design. *Medium*. [online] Disponible en: <https://medium.com/a-parede/questioning-the-critical-in-speculative-critical-design-5a355cac2ca4#.snuht1qbq>
[Fecha de consulta: 4 de noviembre del 2016].

Project Seen, n.d. *Project Seen*. [Online] Disponible en: <http://projectseen.com> [Fecha de consulta: 26 de julio del 2016].

Maass, P., 2014. Art in a Time of Surveillance. *The Intercept*, [online] Disponible en:
<https://theintercept.com/2014/11/13/art-surveillance-explored-artists/>
[Fecha de consulta: 11 de junio del 2016].

Malpass, M., 2013. Between Wit and reason: defining associative, speculative, and critical design in practice. *Design and Culture*, 5(3), pp. 333-356.

Manzini, E., 2015. *Qué es diseño cuando todo el mundo diseña. El diseño en la era de la red (y la sostenibilidad)*. [video Online] Disponible en: <https://www.youtube.com/watch?v=56vfqmpo8k0> [Fecha de consulta: 12 de mayo del 2016].

Manzini, E., Coad, R., 2015. *Design, when everybody designs: An introduction to design for social innovation*. Cambridge: The MIT Press.

Manzini, E., 2016. Design Culture and Dialogic Design. *Design Issues*, 32(1), pp. 52-59.

Mattelart, A., 2002. *Historia de la sociedad de la información.* Barcelona: Paidos.

Mattelart, A., Vitalis, A., 2015. *De Orwell al cibercontrol*. Barcelona: Editorial Gedisa.

Mazé, R., 2014. Forms and Politics of Design Futures. [pdf] *Architecture in Effect, Architecture in the Making and ResArc symposium. Göteborg, apr.*

Mazé, R., Redström, J., 2009. Difficult forms: Critical practices of design and research. *Research Design Journal,* 1(1), pp. 28-39.

McCarthy, S. J., 2013. *The Designer As... Author, Producer, Activist, Entrepreneur, Curator & Collaborator: New Models for Communicating*. Amsterdam: Bis Publishers.

Metaflop, n.d. *Metaflop*. [Online] Disponible en: <http://www.metaflop.com> [Fecha de consulta: 22 de agosto del 2016].

Metahaven, 2015. *Black Transparency. The Right to Know in the Age of Mass Surveillance.* Berlín: Sternberg Press.

Mun, S., 2013. Making Democracy Legible: A Defiant Typeface. *Blog Walker Art Center,* [blog] 20 de junio. Disponible en: <http://blogs.walkerart.org/design/2013/06/20/sang-mun-de-fiant-typeface-nsa-privacy>
[Fecha de consulta: 13 de julio del 2016].

Mun, S., n.d. *ZXX*. [Online] Disponible en: <http://www.sang-mun.com/ZXX-2>
[Fecha de consulta: 26 de julio del 2016].

Museo Nacional Centro de Arte Reina Sofía, 2015. *Duty-Free Art. Hito Steyerl*. [pdf] Museo Nacional Centro de Arte Reina Sofía. Disponible en: <http://www.museoreinasofia.es/sites/default/files/notas-de-prensa/dossier_hito_steyerl.pdf>
[Fecha de consulta: 2 de agosto del 2016].

Samuel, L., 2005. *Disinter: Visual Encryption*. [Online] Disponible en: <http://samluescher.net/projects/disinter-visual-encryption/>
[Fecha de consulta: 21 de noviembre del 2016].

Saxelby, R., 2016. Metahaven Is Breaking The Propaganda Machine. *Fader*, [Online] 6 de mayo. Disponible en: <http://www.thefader.com/2016/05/06/metahaven-the-sprawl-propaganda-interview>
[Fecha de consulta: 6 de mayo del 2016].

Secondthoughts., n.d. *Fundación Alumnos 47* [Online] Disponible en: <http://secondthoughts.mx>
[Fecha de consulta: 4 de noviembre del 2016].

Simon, T., 2015. *Cryptex Typeface*. [Online] Disponible en: <https://www.behance.net/gallery/27696055/Cryptex-Typeface-FREE-FONT> [Fecha de consulta: 21 de noviembre del 2016].

Sinister, D., 2011. A Note on the Type. *Afterall: A Journal of Art, Context and Enquiry*, (27), pp. 28-36.

Soler, J. R., n.d. *La Criptología Española hasta el final de la Guerra Civil.* [pdf] Disponible en: http://www.criptohistoria.es/files/historia.pdf
[Fecha de consulta: 26 de mayo del 2016].

Stein, S. V., 2013. *Black Transparency - The Right To Know In The Age Of Mass Surveillance*. [pdf] Bureau Europa. Disponible en: <http://www.bureau-europa.nl/documents/metahaven_BT_handout.pdf> [Fecha de consulta: 3 de agosto del 2016].

Stein, S. V., 2016. *The Next Big Thing is Not a Thing*. [pdf] Bureau Europa. Disponible en: <http://www.bureau europa.nl/documents/design%20antro_cat%20 cont_online.pdf> [Fecha de consulta: 5 de agosto del 2016].

Sunda, M., 2015. Ruben Pater: Current advancements in drone technology are worrying. *The Japan Times Culture.* [online] Disponible en: <http://www.japantimes.co.jp/culture/2015/02/05/arts/ruben-pater-current-advancements-in-drone-technology-are-worrying/#.V8h-caWU4eLE> [Fecha de consulta: 24 de mayo del 2016].

Sueda, J., 2014. *All possible futures.* London: Bedford Press.

Rubio, D.S., 2016. Crítica a la vigilancia masiva: Metahaven. *Grafica*, 4(8), pp. 117-122.

Regine, 2015. Drones, pirates, everyday racism. An interview with graphic designer Ruben Pater. *We Make Money Not Art*. [online] Disponible en: <http://we-make-money-not-art.com/interview_with_ruben_pater-2/> [Fecha de consulta: 24 de mayo del 2016].

Renza, D., Ballesteros L., Dora M., & Rincón, R., 2016. Método de ocultamiento de píxeles para esteganografía de imágenes en escala de gris sobre imágenes a color. *Ingeniería y Ciencia*. [Online] Disponible en: <https://dx.doi.org/10.17230/ingciencia.12.23.8> [Fecha de consulta: 22 de junio del 2016].

Unicode, n.d. *Unicode.* [Online] Disponible en: <http://www.unicode.org/history/summary.html> [Fecha de consulta: 1 de agosto del 2016].

Whitson, R., 2016. *Review of Benjamin Bratton's The Stack: On Software and Sovereignty*. [Online] Disponible en:
<http://www.rogerwhitson.net/?p=3501>
[Fecha de consulta: 4 de noviembre del 2016]

Whittaker, Z., 2011. Summary: ZDNet's USA PATRIOT Act series. *ZDNET*. [online], Disponible en:
<http://www.zdnet.com/blog/ igeneration/summary-zdnets-usa-patriot-act-series/9233>
[Fecha de consulta: 10 de mayo del 2016].

ZXX., n.d. *ZXX*. [Online] Disponible en: http://z-x-x.org
[Fecha de consulta: 26 de julio del 2016].